OIPE JUL 0 5 2005 JC88 PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: TETSUYA SHIROGANE Application No.: 10/765,289 Filed: January 26, 2004 For: STORAGE APPARATUS AND ACCESS MANAGEMENT METHOD THEREFOR Customer No.: 20350	Examiner: Unassigned Technology Center/Art Unit: 2131 Confirmation No.: 2560 **RENEWED PETITION TO MAKE SPECIAL FOR NEW APPLICATION UNDER M.P.E.P. § 708.02, VIII & 37 C.F.R. § 1.102(d)**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Decision dated May 16, 2005 dismissing the original petition to make special, Applicants respectfully submit a renewed petition to make special the above-identified application under MPEP § 708.02, VIII & 37 C.F.R. § 1.102(d). The application has not received any examination by an Examiner.

(a) The Commissioner has previously been authorized to charge the petition fee of $130 under 37 C.F.R. § 1.17(i) and any other fees associated with this paper to Deposit Account 20-1430.

(b) All the claims are believed to be directed to a single invention. If the Office determines that all the claims presented are not obviously directed to a single invention, then Applicants will make an election without traverse as a prerequisite to the grant of special status.

(c) Pre-examination searches were made of U.S. issued patents, including a classification search, a foreign patent database search, and a literature search. The searches were performed on or around January 10, 2005, and were conducted by a professional search firm, Mattingly, Stanger & Malur, P.C. The classification search covered Class 707 (subclass

1), Class 709 (subclasses 217, 219, 223, and 226), and 711 (subclasses 114 and 152). Because of the large size of these subclasses, keywords were used to narrow of number of documents returned. The foreign patent database search was conducted using Espacenet database and Japanese patent database. The inventors further provided two references considered most closely related to the subject matter of the present application (see references #7-8), which were cited in the Information Disclosure Statement filed on January 26, 2004.

(d) The following references, copies of which were previously submitted, are deemed most closely related to the subject matter encompassed by the claims:

(1) U.S. Patent No. 6,363,067 B1;

(2) U.S. Patent Publication No. 2002/0174307 A1;

(3) U.S. Patent Publication No. 2003/0177239 A1;

(4) U.S. Patent Publication No. 2003/0229690 A1;

(5) U.S. Patent Publication No. 2004/0044744 A1;

(6) U.S. Patent Publication No. 2004/0111391 A1;

(7) Japanese Patent Publication No. JP 2001-265655; and

(8) Japanese Patent Publication No. JP 10-333839.

(e) Set forth below is a detailed discussion of references which points out with particularity how the claimed subject matter is distinguishable over the references.

A. Claimed Embodiments of the Present Invention

The claimed embodiments relate to security management in a storage system allowing a host computer to make accesses to data stored in a storage apparatus.

Independent claim 1 recites a storage apparatus for processing a command transmitted by a host computer connected to the storage apparatus by a network. The storage apparatus comprises a storage unit for storing data to be processed in accordance with the command; a memory for holding an access management table for storing first information on identification of the host computer; a first determination means for determining whether or not a frame of a login request transmitted by the host computer includes second information on identification of the host computer; a request means for transmitting a request to a source

address specified in the frame of the login request in order to request the host computer to transmit the first information on identification of the host computer in a case where the determination result output by the first determination means indicates that the frame of the login request does not include the desired second information; and a second determination means for carrying out a determination process on the first information transmitted by the host computer in response to the request issued by the request means by examination of the access management table. A decision as to whether or not to approve the login request is made in accordance with the determination result output by the second determination means.

Independent claim 10 recites an access control management method for managing an access permit for an access request transmitted by an external apparatus to a storage apparatus by way of a network. The access control management method comprises receiving a frame of a login request from the external apparatus in the storage apparatus; determining whether or not the received frame includes second information for identifying the external apparatus in a first determination process; requesting acquisition of first information for identifying the external apparatus from the external apparatus in a case where a result of the first determination process indicates that the frame does not include the second information; checking the acquired first information in a second determination process in order to determine whether or not an access permit should be given to the external apparatus; and approving an access request made by the external apparatus as a request for an access to the storage apparatus in a case where a result of the second determination process indicates that an access permit should be given to the external apparatus.

Independent claim 20 recites a command-processing method for carrying out a communication between a first apparatus having an iSCSI initiator and a second apparatus having an iSCSI target through an IP network. The command-processing method comprises receiving a frame of a login request made by the first apparatus in the second apparatus; checking whether or not the frame includes first predetermined information for identifying the first apparatus; issuing a request from the second apparatus for acquisition of second predetermined information for identifying the first apparatus from the first apparatus in a case where the frame does not include the first predetermined information; checking whether or not an access made by the first apparatus is to be permitted by examination of the second predetermined information transmitted by the first apparatus to the second apparatus; and processing a command transmitted by the first apparatus to the second apparatus in the iSCSI

target of the second apparatus in a case where a result of checking indicates that an access made by the first apparatus as an access to the second apparatus is permitted.

Independent claim 22 recites a storage apparatus for executing a command received from a host computer connected to the storage apparatus by an IP network. The storage apparatus comprises a storage unit configured to store data to be processed by execution of the command; a memory configured to hold an access management table for storing first information on identification of the host computer; and a processing unit configured to process a request received from the host computer. The processing unit carries out a first determination process to determine whether or not a frame of a login request received from the host computer includes second information on identification of the host computer; transmits a request to a source address specified in the frame of the login request in order to request the host computer to transmit first information on identification of the host computer, and carries out a second determination process on first information transmitted by the host computer in response to the request by examination of the access management table in a case where a determination result output by the first determination process indicates that the frame of the login request does not include desired second information; and makes a decision as to whether or not to approve the login request in accordance with a determination result output by the second determination process.

One of the benefits that may be derived is that it manages accesses by improving security with regard to requests made by a host to make accesses to a storage apparatus adopting the iSCSI protocol.

B. Discussion of the References

1. U.S. Patent No. 6,363,067 B1

This reference discloses a staged partitioned communication bus for a multi-port bridge for a local area network. The communication bus is partitioned into a plurality of data bus segments. Each data bus segment is coupled to one or more ports of the multi-port bridge, and includes a same number (n) of signal lines. A staging multiplexer is coupled to each data bus segment and to a memory device. A bus controller is coupled to each port and to the multiplexer. Each port requests access to the memory device from the bus controller for storing data packets in the memory device and for retrieving data packets therefrom. In response to such requests, the bus controller conditions the multiplexer to provide a signal

path between the memory device and the data bus segment that includes the requesting port. A look-up bus included in the multi-port bridge, which is operable independently of the staged partitioned bus, is preferably coupled to each port of the multi-port bridge and to a look-up table. The look-up table correlates destination addresses for data packets to identifications of destination ports. See, e.g., Abstract; Figures 1-22; and column 2, line 22 to column 3, line 55, and column 6, lines 20-49.

The reference does not teach determining whether or not a frame of a login request transmitted by an apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) includes information (second information in claims 1, 10, and 22; or first predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20); and requesting the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) to transmit additional information (first information in claims 1, 10, and 22; or second predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) if the frame of the login request does not include the desired information, as recited in independent claims 1, 10, 20, and 22.

2. U.S. Patent Publication No. 2002/0174307 A1

This reference shows a method for controlling secure access to storage devices attached to computer system networks. The system includes: a data storage device having the capability of comprising more than one storage structure; a switch comprising more than one port, wherein the ports are individually attachable to separate network systems and wherein the switch has the capability of receiving at one of its ports a request for access to one of the storage structures, and of identifying the network system making the request via the port at which the request was received; and an interface/controller connected to the switch and to the data storage device, wherein the interface/controller has the capability of receiving storage structure access requests from the switch and wherein the interface/controller has the capability of granting access to the storage structure requested if the identified network system making the request has authority to access that storage structure and otherwise has capability of refusing access. The system also includes a port translation table that includes at least one entry comprising the identity of one of the ports and the identity of a virtual local area

network specified as being attached to that port. See, e.g., Abstract; Figures 1-4; and paragraphs [0007]-[0010], [0021], [0038], and [0043].

The reference does not teach determining whether or not a frame of a login request transmitted by an apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) includes information (second information in claims 1, 10, and 22; or first predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20); and requesting the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) to transmit additional information (first information in claims 1, 10, and 22; or second predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) if the frame of the login request does not include the desired information, as recited in independent claims 1, 10, 20, and 22.

3. U.S. Patent Publication No. 2003/0177239 A1

This reference shows a method of managing a resource storage data, storage media having a resource managing program, and a resource manager for managing the resource storage data. The method includes receiving a resources allocation request across the network; converting the received resources allocation request into a setup request for network equipment that exerts control of the network; and sending the setup request to the network equipment or the storage systems across the network. If the resources allocation request designates an asset on an IP network, the request is converted into a setup request including the MAC address of the asset as an API parameter. This may include further steps of: under the control of the resources managing program, registering the following entries into a table: for each unit of the resources of the storage systems, its identifier on the network, its address which adapts to the type of the network, and a group identifier which is assigned by grouping the resources into allocation units; and allocating resources units making up a group in a lump, according to the group identifier. See, e.g., Abstract; Figures 1-9; and paragraphs [0010] and [0022]-[0031].

The reference does not teach determining whether or not a frame of a login request transmitted by an apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) includes information (second information in claims

1, 10, and 22; or first predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20); and requesting the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) to transmit additional information (first information in claims 1, 10, and 22; or second predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) if the frame of the login request does not include the desired information, as recited in independent claims 1, 10, 20, and 22. Nor does it disclose a specific request means for transmitting a request from the external apparatus to a source address specified in the frame of the login request.

4. U.S. Patent Publication No. 2003/0229690 A1

This reference discloses a secure storage system for securely accessing a storage device on a network and improving volume management scalability. The storage system includes a storage device and a client connected to a virtual private network using the storage device. The system further includes: a management apparatus that manages the storage device by means of a logical volume assigned to the storage device; a conversion apparatus that converts a protocol corresponding to the storage device and a protocol used for the virtual private network; and a mapping means that stores a virtual private network allocated to the client and an access range of the storage device corresponding to the virtual private network. An iSCSI interface may be used for an access request from the conversion apparatus to the storage device. See Abstract; Figures 1-27; and paragraphs [0014]-[0019] and [0050]-[0066].

The reference does not teach determining whether or not a frame of a login request transmitted by an apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) includes information (second information in claims 1, 10, and 22; or first predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20); and requesting the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) to transmit additional information (first information in claims 1, 10, and 22; or second predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external

apparatus in claim 10 or first apparatus in claim 20) if the frame of the login request does not include the desired information, as recited in independent claims 1, 10, 20, and 22.

5. U.S. Patent Publication No. 2004/0044744 A1

This reference shows methods, devices and systems for storage management in digital networks. The method provides a switch system having a first and second configurable set of processor elements to process storage resource connection requests, and to route the requests to at least one of the storage elements. Also included is a configurable switching fabric interconnected between the first and second sets of processor elements for: receiving at least a first storage connection request from one of the first set of processor elements; determining an appropriate one of the second set of processors for processing the storage connection request; automatically configuring the storage connection request in accordance with a protocol utilized by the selected one of the second set of processors; and forwarding the storage connection request to the selected one of the second set of processors for routing to at least one of the storage elements. The system has an IP data network including a network management system, a switch element, and at least one remote SCSI device attached to the switch element. A method of automatically discovering the remote SCSI device via the network includes: assigning, in the switch element, an IP address for the remote SCSI device; creating, in the switch element, an address resolution protocol (ARP) table including a table entry for the remote SCSI device; and the ARP table entry providing a mapping between the IP address and a physical address corresponding to the remote SCSI device. See, e.g., Abstract; Figures 1-46; and paragraphs [0017]-[0024], [0074]-[0081], and [0213]-[0216].

The reference does not teach determining whether or not a frame of a login request transmitted by an apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) includes information (second information in claims 1, 10, and 22; or first predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20); and requesting the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) to transmit additional information (first information in claims 1, 10, and 22; or second predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external

apparatus in claim 10 or first apparatus in claim 20) if the frame of the login request does not include the desired information, as recited in independent claims 1, 10, 20, and 22.

6. U.S. Patent Publication No. 2004/0111391 A1

This reference discloses a command processing system by a management agent. In the system an ad hoc program is introduced that runs on a storage subsystem and which, upon receiving a management command from a system management computer, determines whether it should be executed or rejected, judging from the security level of the communication path from/to the system management computer and the security level required for the execution of the command. The system has a memory that stores a first table pre-registering the security levels of the communication path between the management application and the management agent; a first and second means of obtaining, for each command sent from the management application to the management agent, the operational security level for the command by referencing the first and second table; a third means of comparing the operational security level obtained by the first means and the required security level obtained by the second means; and a fourth means of determining whether to permit the execution of the command based on the result of the comparison made by the third means. See, e.g., Abstract; Figures 1-5; and paragraphs [0006]-[0007] and [0042]-[0048].

The reference does not teach determining whether or not a frame of a login request transmitted by an apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) includes information (second information in claims 1, 10, and 22; or first predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20); and requesting the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) to transmit additional information (first information in claims 1, 10, and 22; or second predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) if the frame of the login request does not include the desired information, as recited in independent claims 1, 10, 20, and 22.

7. Japanese Patent Publication No. JP 2001-265655

This reference discloses a technique to provide a security function in a storage subsystem by the flexible and efficient presentation method of storage resources by performing execution by high-speed judgment logic without affecting a processing on the side of a host computer. An information WWN for uniquely identifying the host computer, a management table where the correspondence of a logical unit number LUN inside the storage subsystem for which access is permitted to the host computer and a virtual LUN for presenting the LUN to be the access object to the host computer by a user optional method is described and the management table where the correspondence of the WWN and a dynamically allocated management number S-ID is described are stored in a nonvolatile memory inside the storage subsystem beforehand. By retrieving the WWN of the host computer from the S-ID of the host computer and retrieving the accessible virtual LUN from the WWN, access propriety to the LUN inside the storage subsystem is judged.

In this reference, a relation between WWNs assigned to hosts and port IDs is stored in a table. For a frame including no WWN (e.g., a frame including CDB), the WWN for the port ID is examined to determine whether the host is allowed to make an access to the LU. Present application, at page 3, lines 3-8. In the IP network, however, information may be transmitted by way of a router. In this case, the MAC address included in a datalink frame is replaced with the MAC address of the network card of the router. Thus, if a router exists between the host and the storage apparatus, there is raised a problem that the target is not capable of acquiring the MAC address of the host from a packet received from the host. The reference does not describe a method of acquiring the MAC address of the host in a transmission through a router in the case of an MAC address used as an identification of the host in the IP network. Present application, at page 4, line 14 to page 5, line 1.

The reference does not teach determining whether or not a frame of a login request transmitted by an apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) includes information (second information in claims 1, 10, and 22; or first predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20); and requesting the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) to transmit additional

information (first information in claims 1, 10, and 22; or second predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) if the frame of the login request does not include the desired information, as recited in independent claims 1, 10, 20, and 22.

8. Japanese Patent Publication No. JP 10-333839

This reference discloses a fiber channel connection storage controller having a security function for preventing any illegal access from a host device in an environment in which access from all of host devices can be physically accepted. N Port Name information for uniquely identifying a host device is set in a microprocessor 42 of a storage controller 40 before the starting of host devices 10, 20, and 30. When the host devices 10, 20, and 30 are stated, and an issued frame is received by the storage controller 40, the microprocessor 42 operates comparison to detect whether or not the N Port Name information stored in this frame is registered in an N Port Name list in a control table already set and held in the microprocessor 42, and continues a processing based on the instruction of the frame when they are made coincident, and rejects the request when they are not made coincident. Thus, any illegal access from the host device can be suppressed, and the security can be held.

In this reference, a table is stored in the storage apparatus in advance. For each LU, the table shows WWNs (World Wide Names) each assigned to a host allowed to make accesses to the LU. A WWN stored in a login frame received from a host is compared with those cataloged in the table to identify the host and to determine whether or not the host is allowed to make an access to the LU in the storage apparatus. Present application, at page 2, line 20 to page 3, line 2. In the IP network, however, information may be transmitted by way of a router. In this case, the MAC address included in a datalink frame is replaced with the MAC address of the network card of the router. Thus, if a router exists between the host and the storage apparatus, there is raised a problem that the target is not capable of acquiring the MAC address of the host from a packet received from the host. The reference does not describe a method of acquiring the MAC address of the host in a transmission through a router in the case of an MAC address used as an identification of the host in the IP network. Present application, at page 4, line 14 to page 5, line 1.

The reference does not teach determining whether or not a frame of a login request transmitted by an apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) includes information (second information in claims 1, 10, and 22; or first predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20); and requesting the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) to transmit additional information (first information in claims 1, 10, and 22; or second predetermined information in claim 20) on identification of the apparatus (host computer in claims 1 and 22 or external apparatus in claim 10 or first apparatus in claim 20) if the frame of the login request does not include the desired information, as recited in independent claims 1, 10, 20, and 22.

(f) In view of this petition, the Examiner is respectfully requested to issue a first Office Action at an early date.

Respectfully submitted,

Chun-Pok Leung
Reg. No. 41,405

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 650-326-2400;
Fax: 415-576-0300
RL:rl
60516297 v1